Semifields, Relative Difference Sets, and Bent Functions

Alexander Pott

Otto-von-Guericke-University Magdeburg

December 09, 2013

Outline, or:

Outline, or: Why I am nervous

Outline, or: Why I am nervous

- bent functions ... CLAUDE CARLET, TOR HELLESETH

Outline, or: Why I am nervous

- bent functions ... CLAUDE CARLET, TOR HELLESETH
- relative difference sets (uninteresting generalization?)

Outline, or: Why I am nervous

- bent functions ... CLAUDE CARLET, TOR HELLESETH
- relative difference sets (uninteresting generalization?)
- $\mathbb{Z}_4$ (very old?)

Describe connection between ...

- relative difference sets
- semifields
- projections of relative difference sets
- KNUTH operation on semifields
- bent functions
- $\mathbb{Z}_4$-valued bent functions

The team

- Yue Zhou
- Kai-Uwe Schmidt
- Alex. P.

The team

- YUE ZHOU
- KAI-UWE SCHMIDT
- ALEX. P.

... all this is also related to KATHY HORADAM's work, but less general and more concrete...

Bent functions, even characteristic

- Bent functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ such that $f(x+a) - f(x)$ is balanced for all $a \neq 0$.

Example

$f(x) = \mathrm{Trace}(\beta x^3)$ on $\mathbb{F}_{2^n}$:

$$\begin{aligned} f(x+a) - f(x) &= \mathrm{Trace}(\beta(x^2 a + a^2 x + a^2)) \\ &= \mathrm{Trace}(x^2 \beta(a + \beta a^4) + \beta a^2) \end{aligned}$$

hence $1 + a^3\beta \neq 0$ for all $a \neq 0$.

Necessary condition $n = 2m$ is even.

Bent functions, odd characteristic

- Bent functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ such that $f(x+a) - f(x)$ is balanced for all $a \neq 0$.

Example

$f(x) = \mathrm{Trace}(\beta x^2)$:

$$f(x+a) - f(x) = \mathrm{Trace}(2x\beta a) + \beta a^2.$$

Any n.

Vectorial versions, even characteristic

- Bent functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^k$ such that $F(x+a) - F(x)$ is balanced for all $a \neq 0$.

  Component functions $\mathrm{Trace}(\beta F(x))$ are bent.

  Hence: Vector space of bent functions.

  Necessary condition $n = 2m$ is even and $k \leq m$.

Example

$$F(x, y) = xy$$

$(x, y \in \mathbb{F}_{2^m})$ is vectorial bent $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$

Vectorial versions, odd characteristic

- Bent functions $F : \mathbb{F}_p^n \to \mathbb{F}_p^k$ such that $F(x+a) - F(x)$ is balanced for all $a \neq 0$.

  Component functions $\mathrm{Trace}(\beta F(x))$ are bent.

  Hence: Vector space of bent functions.

  Necessary condition $k \leq n$.

Example

$F(x) = x^2$:

$$F(x+a) - F(x) = 2xa + a^2.$$

$F : \mathbb{F}_p^n \to \mathbb{F}_p^k$ bent

$p = 2$	p odd
n even and $k \leq \frac{n}{2}$	$k \leq n$

$k = n$: planar functions

Bent functions and relative difference sets

If $F : \mathbb{F}_p^n \to \mathbb{F}_p^k$ is bent, the set

$$G_F := \{(x, F(x)) \ : \ x \in \mathbb{F}_p^n\} \subseteq \mathbb{F}_p^n \times \mathbb{F}_p^k$$

is a relative difference set:

Bent functions and relative difference sets

If $F : \mathbb{F}_p^n \to \mathbb{F}_p^k$ is bent, the set

$$G_F := \{(x, F(x)) \ : \ x \in \mathbb{F}_p^n\} \subseteq \mathbb{F}_p^n \times \mathbb{F}_p^k$$

is a relative difference set:

Every element outside $\{0\} \times \mathbb{F}_p^k$ has the same number of difference representations $g = d - d'$ with $d, d' \in G_F$:

$$x - y = a, \quad F(x) - F(y) = b$$

is equivalent to

$$F(y + a) - F(y) = b$$

Other groups?

- group G
- subgroup N (forbidden subgroup)
- subset D

$g \in G \setminus N$ has constant number of representations $g = d - d'$ with $d, d' \in D$, no element in N.

Example

$D = \{1, 2, 4\} \subseteq \mathbb{Z}_8$, forbidden subgroup $\{0, 4\}$.

In this talk: $|D| = \frac{|G|}{|N|}$, hence from each coset of N exactly one element.

The projection construction

If $U < N$ is a normal subgroup of G and D relative difference set, then

$$D/U$$

is a relative difference set in

$$G/U$$

with forbidden subgroup

$$N/U.$$

The size is

$$|D/U| = |D|.$$

One relative difference set produces a chain of relative difference sets.

Planar functions: $n = k$

Definition

A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is planar if $F(x + a) - F(x)$ is a permutation for all $a \neq 0$.

We obtain (vectorial) bent functions via projection.

p must be odd.

Planar functions: $n = k$

Definition

A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is planar if $F(x + a) - F(x)$ is a permutation for all $a \neq 0$.

We obtain (vectorial) bent functions via projection.

p must be odd.

If $p = 2$, then generalize to ??

Two generalizations to characteristic 2

- almost perfect nonlinear functions (APN):
  $F(x+a)-F(x)=b$ has at most 2 solutions.

- relative difference sets in other groups (not elementary abelian), related to semifields.

Two generalizations to characteristic 2

- almost perfect nonlinear functions (APN):
  $F(x+a)-F(x)=b$ has at most 2 solutions.

- relative difference sets in other groups (not elementary abelian), related to semifields.

Dream: Use the many semifields with $p=2$ to construct many APN.

Semifields

$(\mathbb{S}, +, \odot)$ is a finite (pre)semifield (*field without associativity*) if

- $(\mathbb{S}, +)$ is a finite abelian group.
- $x \odot a = b$ has a unique solution x if $a \neq 0$.
- $a \odot y = b$ has a unique solution y if $a \neq 0$.
- $x \odot (y + z) = x \odot y + x \odot z$ and $(x + y) \odot z = x \odot z + y \odot z$.

Example: Finite field!

Semifields

$(\mathbb{S}, +, \odot)$ is a finite (pre)semifield (*field without associativity*) if

- $(\mathbb{S}, +)$ is a finite abelian group.
- $x \odot a = b$ has a unique solution x if $a \neq 0$.
- $a \odot y = b$ has a unique solution y if $a \neq 0$.
- $x \odot (y + z) = x \odot y + x \odot z$ and $(x + y) \odot z = x \odot z + y \odot z$.

Example: Finite field!

- $T_a : \mathbb{S} \to \mathbb{S}$ with $T_a(x) := x \odot a$ is an isomorphism.
- $T_a + T_{a'} = T_{a+a'}$.

Vector space of invertible linear mappings.

$\mathbb{S}$ is elementary abelian (additive group of a field $\mathbb{F}_{p^n}$), multiplication not always commutative.

Why?

Construct projective plane from a semifield:

Why?

Construct projective plane from a semifield:

- Points: $\mathbb{S} \times \mathbb{S}$
- Lines: $\{x, m \odot x + y \ : \ x \in \mathbb{S}\}$.

How many?

- p odd: quite a few, but not many.
  LAVRAUW, POLVERINO (2012).
- $p = 2$: very many commutative KANTOR (2003).

Question

Number is not bounded by a polynomial.

Semifields and relative difference sets

Any semifield gives rise to a relative difference set in a group of order p^{2n} with forbidden subgroup of order p^n:

Semifields and relative difference sets

Any semifield gives rise to a relative difference set in a group of order p^{2n} with forbidden subgroup of order p^n:

Consider the set $\mathbb{S} \times \mathbb{S}$ with addition $\oplus$

$$(a, b) \oplus (a', b') = (a + a', b + b' + a \odot a').$$

Semifields and relative difference sets

Any semifield gives rise to a relative difference set in a group of order p^{2n} with forbidden subgroup of order p^n:

Consider the set $\mathbb{S} \times \mathbb{S}$ with addition $\oplus$

$$(a, b) \oplus (a', b') = (a + a', b + b' + a \odot a').$$

Difference set:

$$\{(a, 0) \ : \ a \in \mathbb{S}\}$$

What are these strange groups?

Let $\mathbb{S}$ be commutative:

- $\mathbb{F}_p^{2n}$ if p is odd,
- $\mathbb{Z}_4^n$ if $p = 2$. Forbidden subgroup: $2\mathbb{Z}_4^n$.

In the p odd case: Planar function.

The KNUTH cube

Basis e_i of $\mathbb{S}$

$$e_i \odot e_j = \sum_k a_{i,j,k} e_k$$

with $a_{i,j,k} \in \mathbb{F}_p$.
Linear mappings are described by matrices

$$(a_{i,k}).$$

Permuting the indices gives **six** semifields (KNUTH).

The KNUTH cube

Basis e_i of $\mathbb{S}$

$$e_i \odot e_j = \sum_k a_{i,j,k} e_k$$

with $a_{i,j,k} \in \mathbb{F}_p$.
Linear mappings are described by matrices

$$(a_{i,k}).$$

Permuting the indices gives **six** semifields (KNUTH).

If $\mathbb{S}$ is commutative, the linear mappings associated with one of the 6 semifields are symmetric: Vector space of symmetric invertible matrices.

What are the projections of RDS, p odd?

One semifield in Knuth orbit of a commutative semifield is vector space of symmetric invertible matrices, another one can be described by planar function (RDS).

The invertible matrices associated with F

$$x \mapsto F(x+a) - F(x) - F(a) + F(0).$$

are not symmetric.

What are the projections of RDS, p odd?

One semifield in Knuth orbit of a commutative semifield is vector space of symmetric invertible matrices, another one can be described by planar function (RDS).

The invertible matrices associated with F

$$x \mapsto F(x+a) - F(x) - F(a) + F(0).$$

are not symmetric.

p odd: Symmetric invertible matrix $(a_{i,j})$ gives a bent function

$$f(x_1, \ldots, x_n) = \sum_{i,j} a_{i,j} x_i x_j.$$

These are the projections of the planar function F!

What are the projections of RDS, p odd?

One semifield in Knuth orbit of a commutative semifield is vector space of symmetric invertible matrices, another one can be described by planar function (RDS).

The invertible matrices associated with F

$$x \mapsto F(x+a) - F(x) - F(a) + F(0).$$

are not symmetric.

p odd: Symmetric invertible matrix $(a_{i,j})$ gives a bent function

$$f(x_1, \ldots, x_n) = \sum_{i,j} a_{i,j} x_i x_j.$$

These are the projections of the planar function F!

Nice representation of KNUTH operation in terms of relative difference sets.

$p = 2$: Difference set in $\mathbb{Z}_4^n$

KNUTH gives invertible symmetric matrices $(a_{i,j})$.

Projections are relative difference set in the group $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$.

$p = 2$: Difference set in $\mathbb{Z}_4^n$

KNUTH gives invertible symmetric matrices $(a_{i,j})$.

Projections are relative difference set in the group $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$.

The group defined on the set $\mathbb{Z}_2^n \times \mathbb{Z}_2$ with addition

$$(v, x) \oplus (w, y) = (v + w, x + y + \sum_i a_{i,i} v_i w_i)$$

is $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$.

$p = 2$: Difference set in $\mathbb{Z}_4^n$

KNUTH gives invertible symmetric matrices $(a_{i,j})$.

Projections are relative difference set in the group $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$.

The group defined on the set $\mathbb{Z}_2^n \times \mathbb{Z}_2$ with addition

$$(v, x) \oplus (w, y) = (v + w, x + y + \sum_i a_{i,i} v_i w_i)$$

is $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$.
The set

$$\{(\mathbf{x}, \sum_{i<j} a_{i,j} x_i x_j) \ : \ \mathbf{x} \in \mathbb{Z}_2^n\}$$

is a projection RDS in that group.

The group $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$

Consider the set $\mathbb{Z}_2^n \times \mathbb{Z}_2$ and define addition

$$(v, x) \oplus (w, y) = (v + w, x + y + \langle v, w \rangle)$$

The group $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$

Consider the set $\mathbb{Z}_2^n \times \mathbb{Z}_2$ and define addition

$$(v, x) \oplus (w, y) = (v + w, x + y + \langle v, w \rangle)$$

If $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$, then

$$G_f := \{(x, f(x)) \ : \ x \in \mathbb{Z}_2^n\}$$

is a relative difference set in $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$ if and only if

$$f(x + a) + f(x) + \langle x, a \rangle$$

is balanced for all $a \neq 0$.

The group $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$

Consider the set $\mathbb{Z}_2^n \times \mathbb{Z}_2$ and define addition

$$(v, x) \oplus (w, y) = (v + w, x + y + \langle v, w \rangle)$$

If $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$, then

$$G_f := \{(x, f(x)) \ : \ x \in \mathbb{Z}_2^n\}$$

is a relative difference set in $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$ if and only if

$$f(x + a) + f(x) + \langle x, a \rangle$$

is balanced for all $a \neq 0$.
Character theoretic characterization:

$$\left| \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x,a \rangle + f(x)} i^{w(x)} \right|^2 = 2^n$$

negabent.

Construction of difference sets in $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$

Theorem ( )

D, E difference sets in G. Then

$$\{0\} \times D \cup \{1\} \times E \cup \{2\} \times (G \setminus D) \cup \{3\} \times (G \setminus E)$$

is a relative difference set in $\mathbb{Z}_4 \times G$ relative to $2\mathbb{Z}_4 \times \{0\}$.

Start with bent function difference sets.

If $G = \mathbb{Z}_2^{n-1}$: negabent (equivalently $\mathbb{Z}_4$-valued bent).

Construction of difference sets in $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$

Theorem (Arasu, Jungnickel, Ma, P.)

D, E difference sets in G. Then

$$\{0\} \times D \cup \{1\} \times E \cup \{2\} \times (G \setminus D) \cup \{3\} \times (G \setminus E)$$

is a relative difference set in $\mathbb{Z}_4 \times G$ relative to $2\mathbb{Z}_4 \times \{0\}$.

Start with bent function difference sets.

If $G = \mathbb{Z}_2^{n-1}$: negabent (equivalently $\mathbb{Z}_4$-valued bent).

Construction of difference sets in $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$

Theorem (Arasu, Jungnickel, Ma, P. (1990))
D, E difference sets in G. Then

$$\{0\} \times D \cup \{1\} \times E \cup \{2\} \times (G \setminus D) \cup \{3\} \times (G \setminus E)$$

is a relative difference set in $\mathbb{Z}_4 \times G$ relative to $2\mathbb{Z}_4 \times \{0\}$.

Start with bent function difference sets.

If $G = \mathbb{Z}_2^{n-1}$: negabent (equivalently $\mathbb{Z}_4$-valued bent).

If you want to find new objects related to RDS's, look at

- Bernhard Schmidt's thesis
- Davis/Jedwab

Another look at RDS in $\mathbb{Z}_4^n$

Consider the set $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ with addition

$$(x, y) \oplus (x', y') = (x + x', y + y' + x \cdot x').$$

Group: $\mathbb{Z}_4^n$, and $\{(0, y) : y \in \mathbb{F}_{2^n}\}$ is elementary abelian subgroup.

Another look at RDS in $\mathbb{Z}_4^n$

Consider the set $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ with addition

$$(x, y) \oplus (x', y') = (x + x', y + y' + x \cdot x').$$

Group: $\mathbb{Z}_4^n$, and $\{(0, y) : y \in \mathbb{F}_{2^n}\}$ is elementary abelian subgroup.

Question

Which subsets

$$\{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$$

are relative difference sets.

Another look at RDS in $\mathbb{Z}_4^n$

Consider the set $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ with addition

$$(x, y) \oplus (x', y') = (x + x', y + y' + x \cdot x').$$

Group: $\mathbb{Z}_4^n$, and $\{(0, y) : y \in \mathbb{F}_{2^n}\}$ is elementary abelian subgroup.

Question

Which subsets

$$\{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$$

are relative difference sets.

Theorem (Zhou (2012))

Relative difference set if and only if

$$F(x + a) - F(x) + a \cdot x$$

is a permutation for all $a \neq 0$.

Such an F is called planar.

ridiculous example

$$F(x) = 0$$

ridiculous example

$$F(x) = 0$$

$$F(x + a) + F(x) + a \cdot x = a \cdot x$$

is a permutation for all $a \neq 0$.

Many semifields

Thanks to KANTOR (2003): There are many semifields!

Many semifields

Thanks to KANTOR (2003): There are many semifields!

Theorem

$\mathbb{K} = \mathbb{K}_0 \supset \mathbb{K}_1 \supset \cdots \supset \mathbb{K}_n$ of characteristic 2 with $[\mathbb{K} : \mathbb{K}_n]$ odd. Let tr_i be the relative trace from $\mathbb{K}$ to $\mathbb{K}_i$. Then, for all nonzero $\zeta_1, \ldots, \zeta_n \in \mathbb{K}$, the mapping $F : \mathbb{K} \to \mathbb{K}$ given by

$$F(x) = \left(x \sum_{i=1}^{n} \mathrm{tr}_i(\zeta_i x) \right)^2$$

is planar. Examples are inequivalent.

Construction of new commutative semifields

- New symplectic spreads (symmetric invertible matrices) (Italian school)
- New planar functions (German-Chinese-Norwegian-Armenian school)

The COULTER-MATTHEWS (1998) example

The only known planar function not corresponding to semifields:

Theorem

The function $F(x) = x^d$ *with*

$$d = \frac{3^a + 1}{2}$$

is PN in $\mathbb{F}_{3^n}$ *iff* $\gcd(a, n) = 1$ *and* a *odd.*

The COULTER-MATTHEWS (1998) example

The only known planar function not corresponding to semifields:

Theorem

The function $F(x) = x^d$ *with*

$$d = \frac{3^a + 1}{2}$$

is PN in $\mathbb{F}_{3^n}$ *iff* $\gcd(a, n) = 1$ *and* a *odd.*

p even???

Switching

Planar function such that image set of F has size 2?

Theorem (Zhou 2012)

Switching

Planar function such that image set of F has size 2?

Theorem (Zhou 2012)

No

Power mappings $F(x) = \alpha \cdot x^d$

$F(x + a) - F(x) + a \cdot x$ permutation.

Power mappings $F(x) = \alpha \cdot x^d$

$F(x+a) - F(x) + a \cdot x$ permutation.

Known power mappings αx^d which are planar:

d	condition	
2^k	no	folklore
$2^k + 1$	$n = 2k$	SCHMIDT, ZHOU
$4^k(4^k + 1)$	$n = 6k$	SCHERR, ZIEVE

Power mappings $F(x) = \alpha \cdot x^d$

$$F(x+a) - F(x) + a \cdot x \quad \text{permutation.}$$

Known power mappings αx^d which are planar:

d	condition	
2^k	no	folklore
$2^k + 1$	$n = 2k$	SCHMIDT, ZHOU
$4^k(4^k + 1)$	$n = 6k$	SCHERR, ZIEVE

Theorem (MÜLLER, ZIEVE (2013))

Let d be a positive integer such that $d^4 \leq 2^m$ and let $c \in \mathbb{F}_{2^m}$ be nonzero. Then the function $x \mapsto \alpha x^d$ is planar on $\mathbb{F}_{2^m}$ if and only if d is a power of 2.

Conclusion

- Semifields give RDS (old result)
- In the commutative case, projections give KNUTH operation (new to me)
- $\mathbb{Z}_4$ valued bent functions have been studied before (new)
- Non-commutative case? (work in progress)
- $p = 2$ Planar functions of low weight (ZHOU)
- $p = 2$ Power planar? (ZHOU, SCHMIDT, ZIEVE, MÜLLER, SCHERR)
- $p = 2$ RDS not semifield (Open)

Epilogue: My dream

Use KANTOR to construct many APN.

Epilogue: My dream

Use KANTOR to construct many APN.

Almost true, but the generalization lives on the wrong face of KNUTH cube (DEMPWOLFF, KANTOR (2013)).